Layered Decoding of Quantum LDPC Codes

Julien Du Crest^{*}, Francisco Garcia-Herrero[†], Mehdi Mhalla[‡], Valentin Savin [§]and Javier Valls [¶]

August 28, 2023

Abstract

We address the problem of doing message passing based decoding of quantum LDPC codes under hardware latency limitations. We propose a novel way to do layered decoding that suits quantum constraints and outperforms flooded scheduling, the usual scheduling on parallel architectures. A generic construction is given to construct layers of hypergraph product codes. In the process, we introduce two new notions, *t-covering layers* which is a generalization of the usual layer decomposition, and a modified scheduling called *random order scheduling*. Numerical simulations show that the random ordering is of independent interest as it helps relieve the high error floor typical of message passing decoders on quantum codes for both layered and serial decoding without the need of post-processing.

1 Introduction

A lot of work has been done in order to improve the decoding of quantum low-density parity-check (qLDPC) codes using message-passing (MP) decoders. Most of these works rely on the use of post-processing techniques [1–3], whose feasibility is still to be demonstrated on actual hardware, due to the stringent latency, power and scalability requirements of the quantum system. A key attribute of MP decoding is the underlying *scheduling*, indicating the order in which variable and check node messages are updated. This has been subject to extensive research in the classical LDPC decoding literature, and it has been shown that the MP scheduling may significantly impact the convergence speed [4], the decoding performance (*e.g.*, in case of adaptive scheduling strategies [5–7]), or the performance (*e.g.*, latency, area, powerconsumption) of the hardware design [8]. The vast majority of hardware designs are

^{*}Univ. Grenoble Alpes, Grenoble INP, LIG, F-38000 Grenoble, France (julien.du-crest@univ-grenoble-alpes.fr)

[†]Department of Computer Architecture and Automatics (DACYA), Complutense University of Madrid, Spain (francg18@ucm.es)

[‡]Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France (mehdi.mhalla@univ-grenoble-alpes.fr)

[§]Univ. Grenoble Alpes, CEA-Léti, F-38054 Grenoble, France (valentin.savin@cea.fr)

[¶]Instituto de Telecomunicaciones y Aplicaciones Multimedia, Universitat Politecnica de Valencia, 46022 Valencia, Spain (jvalls@upv.es)

based on partly-parallel architectures, implementing a layered decoding scheduling, which can be considered as a *de facto* standard solution, able to provide relevant complexity and performance advantages in most applications [8].

For qLDPC codes, the MP decoding performance may depend even more on the underlying scheduling, which can be most likely attributed to the code degeneracy [2]. Moreover, some post-processing techniques may be highly dependent on the MP decoding scheduling. For instance, the order statistics decoding post-processing has been shown to provide very good performance when a layered scheduling is used, but its performance may be drastically degraded using a flooded (*i.e.*, fully parallel) scheduling [2].

To design an *efficient* partly parallel architecture implementing a layered scheduling, one needs a layer decomposition of the parity check matrix. For qLDPC codes this may be tricky, as they do not have an innate decomposition into horizontal layers (as for instance in the case of classical quasi-cyclic LDPC codes). To ensure a high degree of parallelism, it is also desirable to have a decomposition into a minimal number of layers. In this paper, we first give a generic construction of a minimal layer decomposition for hypergraph product codes. Moreover, in an attempt to start bridging the gap between hardware limitations and state of the art MP decoders, we propose two new tools to implement layered decoding of qLDPC codes. The first is a generalization of the notion of layer decomposition, consisting of a family of *t*-covering layers, which can be seen as a layer decomposition of t decoding iterations, and is aimed at increasing the parallelism degree of the layered architecture. The second is a new scheduling called **random order scheduling**, and is shown to significantly improve the decoding performance. Our numerical simulations provide evidence that both could be used in the future to meet hardware needs as they offer a good compromise of speed and performance.

2 Preliminaries

2.1 Quantum Codes

Calderbank-Shor-Steane (CSS) codes are defined by two classical $(m_X/m_Z, n)$ -parity check matrices H_X, H_Z satisfying $H_X H_Z^{\perp} = 0$. The dimension of the quantum code is $n-\operatorname{rank}(H_X)-\operatorname{rank}(H_Z)$ and its minimum distance $d = \{\min |v|, v \in \ker H_X \setminus \operatorname{im} H_Z^t \cup \ker H_Z \setminus \operatorname{im} H_X^t\}$. One such class of CSS codes are the hypergraph product codes (HPC), which given two classical codes A and B give the quantum code $H_X = [A \otimes I, I \otimes B^t]$ and $H_Z = [I \otimes B, A^t \otimes I]$ (see [9] for the construction and parameters of the code).

In the following, we will only focus on decoding Z errors using H_X . All proofs are easily adapted to correcting X errors.

2.2 MP decoding

MP decoders work by exchanging soft information between check and variable nodes on the Tanner graph representation of the code, trying to converge to a hard decision on the variable nodes that satisfy the syndrome. One crucial factor is to decide in which order messages are exchanged and soft information updated. There are three main decoding scheduling used classically: flooded, in which messages are exchanged simultaneously and soft information updated in parallel, serial, where the graph is updated sequentially going through all the checks one by one, and layered, which lies in between, taking advantage of checks that have a disjoint support to update them in parallel, essentially doing a speed up of serial scheduling at no cost. For more details on classical message passing, refer to [10].

2.3 Layered Scheduling

To avoid memory conflicts in a partly parallel architecture, implementing a layered scheduling, the same memory slot should not be read/written to by two different processing units at the same time. This motivates the following definitions.

Definition 1. A layer is a collection of check-nodes such that any two check-nodes have no neighbouring variable-node in common.

Definition 2. A layer decomposition $L_0 \sqcup \cdots \sqcup L_{k-1}$ is a partition of the set of check-nodes into k layers.

Definition 3. A decomposition is said to be **minimal** if it is impossible to find a decomposition in less layers.

A simple density argument is enough to state the following fundamental inequality:

Lemma 1. Any k layers decomposition of a $(_, \delta)$ -regular¹ (m, n)-parity-check matrix satisfies $k \geq \frac{\delta m}{n}$.

Definition 4. A decomposition is γ -balanced if

$$\frac{|L_i|}{|L_i|} \le \gamma, \quad \forall L_i, L_j$$

A decomposition will be said to be **balanced** if it is 1-balanced. Balanced decompositions ensure an efficient use of hardware resources (check-node processing units).

3 Hardware Requirements

In contrast to classical LDPC decoders, which prioritize optimizing throughput, qLDPC ones must satisfy highly constrained values of latency to avoid the backlog problem [11], which would lead to an exponential slowdown of the quantum processor making the QEC implementation impractical.

Table 1: Latency approximation for the different architectures

ParallelSerialLayered
$$T_{min}^{(P)} \times 2 \times it_{max}$$
 $T_{min}^{(S)} \times (it_{max}/2) \times m$ $T_{min}^{(L)} \times 2 \times (it_{max}/2) \times k$

To illustrate the behavior of the decoder, the B1 code from [1] is taken as an example (defined in Section 4). An MP decoder for the B1 code can achieve with

¹A matrix is said to be (c, d)-regular if every column is of weight c and every row of weight d.

this architecture², a clock period between 8 and 10ns which derives a latency between 480ns and 600ns at 30 iterations, that is close to the most constrained technology. Taking this into account, the clock period usually can be reduced to 70% and 80%of the clock period obtained with the parallel version. The question is that with this schedule and the derived architecture only one check node is updated in a clock cycle, because of the sequential update of the messages. Due to this, at least m clockcycles are required 3 to complete just one iteration of the MP algorithm. Following the example of code B1, the clock period should be between 5.6 and 7ns, but the total latency at 30 iterations would be between 74.26μ s and 92.82μ s. Even assuming a reduction of the number of iterations to get similar performance to the flooded schedule, the range of latencies would be out of the time budget of supercomputing qubits and transmons. To meet the timing requirements, the clock period should be equal to $\frac{5.6}{m/2} = 0.025$ ms, which is a maximum clock frequency of 40GHz. This frequency cannot be achieved by any FPGA or ASIC, and on the other hand, it would require a large power consumption that will cause another problem with the power budget and the refrigeration system [13]. With the previous examples, it is easy to conclude that the implementation of serial scheduling, even if it has a better performance than the flooded one, it is not a realistic solution when it comes to implementation. A trade-off solution between both serial and flooded may be the layered schedule. If the number of layers is small enough, the number of clock cycles per iteration will not grow too much and the number of iterations will be usually reduced by two. Going back to the B1 code example, assuming that in the worst case, the clock period will be similar to the parallel architecture, and with a distribution of 3.5 layers⁴ the total latency for 30 iterations will be between $8x3.5x2x30=1.68\mu$ s and $10x3.5x2x30=2.10\mu$ s; and between 8x3.5x2x15 = 840 ns and $10x3.5x2x15 = 1.05\mu$ s with 15 iterations, which is fairly close to the constraints of superconducting qubits and meets the requirements of other technologies.

As we will see in the following sections, the layered schedule will also benefit from some non-negligible performance improvements, apart from the reduction in the number of iterations, compared to the flooded schedule.

In table 1, we can find a summary of the total latency for different architectures, where $T_{min}^{(P)}$, $T_{min}^{(S)}$ and $T_{min}^{(L)}$ are the minimum clock periods achievable by the parallel, serial and layered architectures respectively, and it_{max} is the maximum number of iterations configured in the parallel decoder. Note that we assume that the number of iterations of serial and layered is usually half the number of iterations of the parallel architecture [4].

 $^{^{2}}$ All figures reported here come from our implementation of an either fully parallel [12] or serial min-sum decoder architecture, with exchanged messages quantized on 6 bits, on a Xilinx FPGA xcv095 board.

 $^{^{3}}$ Assuming that due to the reduced complexity of the units both the check node and the connected variable nodes can be updated in parallel.

⁴See Section 4 for the formal definition of fractional layer number.

4 Generic Constructions

4.1 Layered Construction for Hypergraph Product Codes

Consider an hypergraph product code defined by two matrices A and B, such that $H_X = [A \otimes I, I \otimes B^t]$ and $H_Z = [I \otimes B, A^t \otimes I]$ [9]. There exist a layer construction from a layer decomposition of A, B, A^t, B^t .

Theorem 1. Given minimal decompositions $A = A_0 \sqcup \cdots \sqcup A_{k_A-1}, B = B_0^t \sqcup \cdots \sqcup B_{k_{Dt}-1}^t$, one can construct a minimal decomposition of H_X in $k = \max(k_A, k_{B^t})$ layers.

A similar theorem can be stated for A^t, B and H_Z with the same proof techniques.

Construction If $k_A \neq k_B$, without loss of generality, suppose $k_A < k_B$. The first step is to add empty layers to A so that $k'_A = k'_B = k$. That is let $A = A_0 \sqcup \cdots \sqcup A_{k_A-1} \sqcup A_{k_A} \cdots \sqcup A_k$ where $A_{k_A} = \cdots = A_k = \emptyset$. Let's label each row of H_X as

$$a \otimes b := [a \otimes e_b, e_a \otimes b], \quad a \in \operatorname{rows}(A), b \in \operatorname{rows}(B^t)$$

In the following we will denote by *left* the sub-matrix $[A \otimes I]$ and *right* the sub-matrix $[I \otimes B^t]$. Create layers $L_0 \ldots L_{k-1}$ such that

$$(a \circledast b) \in L_i \Leftrightarrow \exists j \quad a \in A_j, b \in B_{i+i \mod k}^t \tag{1}$$

By definition, all checks belong to some layer, we now have to check that any two checks in a given layer have disjoint variable nodes support. Suppose that two checks $a \circledast b, a' \circledast b'$ belong to L_i . Case A : a = a'. They do not touch on the left thanks to the tensor product with the identity. Furthermore, it means that $b \neq b'$ but then both belong to B_l^t for some l, so they have disjoint support on the right. Case B,C : $a \neq a'$. They have disjoint support on the right because of the tensor product with the identity. To show that they do not intersect on the left, there are two cases : If aand a' belong to some A_l (case B), then by definition they have disjoint support on the left. If a and a' belong respectively to $A_l, A_{l'}$ with $l \neq l'$ (case C), then it means that $b \in B_{l+i \mod k}^t, b' \in B_{l'+i \mod k}^t$, two distinct classes. Hence even though a and a'might share variable nodes in A, they do not intersect in the tensored version $A \otimes I$. Fig. 1 depicts a simple example of the 3 cases.

Minimality The proof is by contradiction. Assume that there is a decomposition in less than k_{B^t} layers, then one could recover a decomposition for B^t in less than k_{B^t} from a restriction to the $\{a \otimes b, \forall b\}$ positions for any given a. Any decomposition in less than k_A layers would similarly give a decomposition for A from the restriction of H_X to any $\{a \otimes b, \forall a\}$ for a given b. Hence the decomposition in $\max(k_A, k_B^t)$ is minimal for H_X .

Note that the construction is not unique, for example, Equation 1 can be replaced by the following equation where σ is any k-permutation, although this is still not the most generic formula:

$$(a \circledast b) \in L_i \Leftrightarrow \exists j, \quad a \in A_{\sigma(j)}, b \in B_{j+i \mod k}^t$$

$$\tag{2}$$



Figure 1: Small visualization example of proof cases where $A = B^t$

Theorem 2. Given k-layerings for A and B^t , respectively α and β -balanced. Then H_X is γ -balanced with :

Proof. (i) Let $a_0...a_{k-1}$ be the sizes of layers $A_0...A_{k-1}$, and $b_0...b_{k-1}$ the sizes of the layers $B_0^t...B_{k-1}^t$. Then each layer L_l of H_X has size $\sum a_i b_{i+l}$. We also suppose layers of A and B^t are ordered from biggest to smallest hence $a_0 = \alpha a_{k-1}$ and $b_0 = \beta b_{k-1}$. The layer L_0 of size $\sum a_i b_i$ is the biggest layer, a classical proof of that is by contradiction, using the fact that $\forall a \geq c, b \geq d$, $ab + cd \geq ad + bc$. The ratio between any other layer L_j and L_0 is smaller than β since $\beta \sum a_i b_{i+j} > \sum a_i b_0 > \sum a_i b_i$ using the fact that $\forall b_j$, $\beta b_j \geq b_0$ (and similarly for α).

(ii) Suppose A is perfectly balanced. In that case, for any $b \in B^t$, it will appear the same number of times in each layer L_i since the $a \otimes b, \forall a \in A$ will be equally balanced in the layers. Hence the code will be balanced. The same argument holds if B^t is perfectly balanced.

Corollary 2.1. Given a k_A -layering or A, and a $k_B > k_A$ layering for $B^t \beta$ -balanced. Then H_X is γ -balanced with :

 $\gamma \leq \beta$

Proof. Same as above, considering a k_B layering for A by adding empty layers. This new layering is ∞ -balanced.

4.2 Random Ordering

We introduce a decoding technique called random ordering. This technique consists of applying a random order on the layers' application at each decoding step. This is also generalized to serial decoding by considering that each check belongs to its own layer (i.e. k = m). This seemingly anodyne step helps to alleviate the error floor quite dramatically. In addition, further simulations showed us that one does not even have to use a "good" pseudo-random generator to generate the permutation, and this can be done with virtually no cost using a simple congruent generator, a solution that is hardware friendly.

4.3 *t*-Covering of Layers

For many codes, the theoretical bound on k given by a density argument is not tight. However, since for the quantum codes the number of layers is fixed due to latency constraints, it is important to stay as close as possible to the theoretical bound. We introduce a generalization of the layer decomposition called a *t*-covering of (k)layers. We drop the requirement that the layers should be disjoint, and only require that their union taken with multiplicities should cover each check exactly t times. In the following, the parameters of a t-covers will be specified as (t, k, γ) , giving the cover parameters and the balance of the layers. Note that when using t-covers, the usual term of "iteration" becomes ambiguous because it might be the case that the decoder stops while all the checks have not been seen the same number of times. Since by pipelining the process, the syndrome satisfaction could be checked after each layer application adding very low latency, in the following we will often refer to the number of iterated layers (but always specify it when we do so). To quickly compare a *t*-cover with another or with a layer decomposition, it is useful to introduce the **fractional layer number** as $\frac{k}{t}$, intuitively it captures the "average" number of layers the decoder has to process to see each check once. Finally, by concatenating t times the matrix H, it is clear that the density bound of lemma 1 applies to the fractional layer number. As a simple application, for the code B1 given below, we found a (2,7,1)-cover, $\frac{k}{t} = 3.5$. We could also find a (1,4,2) layer decomposition, $\frac{k}{t} = 4$, and the density bound gives us $\frac{k}{t} \ge 3$, since no decomposition in 3 layers is known for the B1 code, our 2-cover sets a new standard in decoding efficiency.

5 Applications on Particular Quantum Codes

5.1 C2 Code

The C2 code is a hypergraph product code generated from a single cyclic matrix (A = B) of generator polynomial $p(x) = 1 + x^2 + x^5$ and length l = 31. Since this cyclic matrix (and its transpose) accepts a decomposition in 5-layers, using the technique from theorem 1, we can construct a 5 layer decomposition for the C2 code. As said earlier about the balancing effect of the procedure, the decomposition used for A, B, A^t, B^t is (1, 5, 2)-cover and it yields a (1, 5, 1.1)-cover for C2. This shows the balancing effect of the procedure, as we go from $\gamma = 2$ to $\gamma = 1.1$. Here are the layers used for the quasicyclic matrix:

It should be noted that in order to improve the latency (at the cost of a more complex construction), we were also able to create a (224, 961, 1)-cover of C2, achieving a fractional layer number of 4.29 and giving close numerical results.

5.2 B1 Code



Figure 2: Comparison of different decoders and scheduling on B1 and C2 codes under Z-noise. In the simulations, we use a perturbated NMS, where each check node message is multiplied by a normalization factor uniformly chosen at random in $\{0.875, 0.9275\}$ at each iteration. This perturbation is important to avoid an errorfloor degradation.

The B1 code is a Generalized Hypergraph Product code (construction given in [1], Appendix) : As such it shares similarities with the Hypergraph Product Codes.

Although we do not have a generic decomposition for this family of codes, some ideas from the hypergraph product theorem apply when creating a cover for the B1 code. The B1 code accepts a 2-cover in 7 layers, hence giving a fractional layer number of 3.5. The layers are as follows :

$$L_i = \{i + 7j \quad \forall j\} \cup \{3 + i + 7j \quad \forall j\}$$

This 2-cover comes from a decomposition of the quasi-cyclic matrix defined by polynomial $p(x) = 1 + x + x^6$ in 7 layers $S_0 \dots S_6$ such that $S_i = \{i + 7j \quad \forall j\}$ which is an obvious decomposition (albeit not minimal) given the generating polynomial. Those layers have the property that the union of any two layers $S_i, S_{i+3 \mod 7}$ is still a valid layer which gives the basis for the layers of the code B1. In fact, those layers are extended to the matrices of H_X, H_Z much in the fashion of what is done with the hypergraph product but with a "twist" as the blocks are quasi-cyclic shifts of identities instead of all identities so one has to be more careful and cannot use the generic formula.

6 Numerical Results

Fig. 2 compares the different decoding techniques proposed on an HGP and Hyperbicycle Codes under Z-noise. We consider Sum-Product (SP) and Normalized Min-Sum (NMS) decoders, with serial, layered and flooded scheduling [10]. When decoding classical codes, using serial scheduling yields a factor two improvement in convergence speed over flooded scheduling. This is not the case in our numerics on quantum codes, as the serial scheduling suffers from a high error floor. This error floor can be virtually eliminated by using a random ordering scheduling. For the flooded scheduling, the number of iterations used is i = 128, for serial i = 64. For the layered scheduling of a $(t, k, _)$ -cover, the layer iteration number $i_{lay} = \lfloor 64 \times \frac{k}{t} \rfloor$. Although we argued before that checking the syndrome after each layer is essentially costless, to do a "fairer" comparison with serial scheduling under random order scheduling we also tried checking the syndrome only after $\lceil \frac{k}{t} \rceil$ layer iterations. We did not include the numerics as the two curves match almost perfectly, making it a non-issue.

On the B1 code, because it is a *t*-cover and not a layer decomposition, we alter the random ordering scheduling a little bit to boost the performances by requiring that the permutation is not chosen uniformly at random, and must satisfy the additional constraint that two successive layers should not share any check. These additional constraints help the decoder to converge faster as processing the same check twice in a row in different layers would not change its soft information.

7 Conclusion

We showed how to implement a layered scheduling for qLDPC codes to meet with the hardware latency limitations. In our numerics, this decoder was more efficient than what could be achieved using similar resources in flooded scheduling which might make it the go to hardware option in the future. We also show that the random order scheduling is a result interesting on its own, as it can be applied to both serial and layered scheduling to alleviate the high error floor of some codes without the need of a post-processing. It should be noted that presently, the best decoders for those codes use some kind of post-processing after message passing, something that was not studied in this paper, as none of the known post-processings can meet the hardware latency considerations. Knowing that our serial scheduling with random ordering already achieves the performances of the Ordered Statistic Decoding (OSD) post-processing on those codes⁵. Finding such hardware friendly post-processing to use with our layered scheduling would be another step in the direction we are aiming for.

Acknowledgement

This work was supported by the QuantERA grant EQUIP (French ANR-22-QUA2-0005-01, and Spain MCIN/AEI/10.13039/501100011033, grant PCI2022-132922), and the Plan France 2030 (ANR-22-PETQ-0006) and by the European Union "NextGenerationEU/PRTR".

References

- [1] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," *Quantum*, vol. 5, p. 585, 2021, arXiv:1904.02703.
- [2] J. Du Crest, M. Mhalla, and V. Savin, "Stabilizer inactivation for messagepassing decoding of quantum LDPC codes," in *IEEE Information Theory Workshop (ITW)*. IEEE, 2022, pp. 488–493.
- [3] N. Raveendran and B. Vasić, "Trapping sets of quantum LDPC codes," Quantum, vol. 5, p. 562, Oct. 2021.
- [4] J. Zhang, Y. Wang, M. P. C. Fossorier, and J. S. Yedidia, "Iterative decoding with replicas," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1644–1663, 2007.
- [5] Y. Mao and A. H. Banihashemi, "Decoding low-density parity-check codes with probabilistic scheduling," *IEEE Communications Letters*, vol. 5, no. 10, pp. 414– 416, 2001.
- [6] V. Savin, "Iterative LDPC decoding using neighborhood reliabilities," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, 2007, pp. 221–225.
- [7] A. I. Vila Casado, M. Griot, and R. D. Wesel, "LDPC decoders with informed dynamic scheduling," *IEEE Trans. on Communications*, vol. 58, no. 12, pp. 3470–3479, 2010.
- [8] E. Boutillon and G. Masera, "Hardware design and realization for iteratively decodable codes," in *Channel coding: Theory, algorithms, and applications*, D. Declercq, M. Fossorier, and E. Biglieri, Eds. Elsevier, 2014, pp. 583–642.

⁵See [2][Sec 4, Fig. 2], error probability should be multiplied by 2/3 to compare the two since the error model is depolarizing noise there.

- [9] J.-P. Tillich and G. Zémor, "Quantum ldpc codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1193–1202, 2013, arXiv:0903.0566.
- [10] V. Savin, "LDPC decoders," in *Channel coding: Theory, algorithms, and applications*, D. Declercq, M. Fossorier, and E. Biglieri, Eds. Elsevier, 2014, pp. 211–260.
- [11] A. Holmes, M. R. Jokar, G. Pasandi, Y. Ding, M. Pedram, and F. T. Chong, "NISQ+: Boosting Quantum Computing Power by Approximating Quantum Error Correction," in *Proceedings of the ACM/IEEE 47th Annual International* Symposium on Computer Architecture, ser. ISCA '20. IEEE Press, 2020, p. 556–569.
- [12] J. Valls, F. Garcia-Herrero, N. Raveendran, and B. Vasić, "Syndrome-based minsum vs OSD-0 decoders: FPGA implementation and analysis for quantum LDPC codes," *IEEE Access*, vol. 9, pp. 138734–138743, 2021.
- [13] Y. Ueno, M. Kondo, M. Tanaka, Y. Suzuki, and Y. Tabuchi, "QECOOL: On-line quantum error correction with a superconducting decoder for surface code," in 2021 58th ACM/IEEE Design Automation Conference (DAC). IEEE, dec 2021.